



COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

June 22, 2005

To: Supervisor Gloria Molina, Chair
Supervisor Michael D. Antonovich, Chair Pro Tem
Supervisor Yvonne B. Burke
Supervisor Zev Yaroslavsky
Supervisor Don Knabe

From: Jon W. Fullinwider
Chief Information Officer

Subject: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
(HIPAA) STATUS REPORT**

The purpose of this report is to provide a summary of County compliance activities with the HIPAA Transaction and Code Sets (TCS) Rule and Security Rule following their compliance deadlines that were October 16, 2003 and April 20, 2005, respectively. The Auditor-Controller is responsible for monitoring and auditing ongoing County department compliance with the HIPAA Privacy Rule following its compliance deadline of April 14, 2004 and is submitting a separate semi-annual status report to your Board.

Under the HIPAA rules and regulations, the County declared itself a "hybrid covered entity" and identified four County departments as covered components that must implement and comply with the provisions of HIPAA. They include:

- Department of Health Services (DHS)
- Department of Mental Health (DMH)
- Department of Probation's Kirby Center
- Sheriff Department's Pharmacy

Only DHS, DMH, and Probation's Kirby Center are subject to TCS Rule regulations, while all four departments were determined to be subject to Security Rule regulations.

The following provides a summary of County HIPAA TCS and information security remediation activities, and key TCS and Security Rule compliance issues. In addition, attached are two charts providing detailed information on County departments' TCS compliance status by transaction (Attachment A) and County department status by each Security Rule standard (Attachment B).

Summary

TCS Rule

County departments' progress towards achieving full TCS compliance is largely unchanged since the last status report. Progress has been limited due to the State's inability to test and implement many required HIPAA transactions. However, the State has recently begun to test the eligibility transaction pair (270/271) for State Department of Mental Health trading partners. While this State movement towards testing and implementing the full HIPAA transaction set is encouraging, this will likely be a slow process.

The Department of Health Services (DHS) through its claims processing clearinghouse, Accordis, is submitting HIPAA compliant Medi-Cal inpatient claims to the State using revenue codes based upon agreements reached with the State governing TCS processing. As previously reported, the State has indicated that they will not be prepared to accept HIPAA compliant Medi-Cal outpatient claims until calendar year 2006. DHS is continuing efforts internally to expand the use of HIPAA compliant transactions with other trading partners.

The Department of Mental Health (DMH) is processing HIPAA-compliant Medi-Cal claim files to the State. The problems with the file size and third-party payers have been resolved and DMH is now current with both inpatient and outpatient claim submissions.

DMH is continuing to address Integrated System (IS) performance, reliability and functionality issues. In response to your Board's November 30, 2004 order, DMH is also submitting a HIPAA-related Board report detailing their activities to improve the performance and reliability of the IS and its use by their providers.

Security Rule

The Security Rule requires that reasonable and appropriate safeguards be implemented to protect the confidentiality, integrity and availability of electronic protected health information (EPHI) by the established compliance date. Affected departments are making continuing progress to comply with the Security Rule, and as reported in the last security status report, the County can document their good faith efforts to implement the 18 security standards identified under the security portion of the regulations.

The Security Risk Analysis, which identifies and assesses risk exposure to EPHI and provides recommendations to reduce risk to a reasonable and appropriate level, is nearing completion. DHS Olive View/UCLA Medical Center, who suspended HIPAA activities to concentrate on its Joint Commission on Accreditation of Healthcare Organizations licensure review, has worked with Fox Systems (FOX), the consultant, to complete its analysis.

Detailed reports have been reviewed with all covered departments and are scheduled to be delivered on July 1, 2005 with the final consolidated report scheduled for delivery on July 15, 2005. When the reports are completed, the covered departments will be

required to develop implementation plans addressing all report findings and recommendations and provide bi-weekly status to the CIO's Chief Information Security Officer (CISO).

TCS Compliance Issues

Department of Health Services

- **HIPAA Compliant Medi-Cal Outpatient Claims.** Accordis, the DHS vendor functioning as the claims clearinghouse, is submitting HIPAA compliant Medi-Cal inpatient claims to the State using appropriate HIPAA compliant UB-92 revenue codes based on agreements reached with the State. On December 2, 2004, the State indicated that they will not be converting the County's Medi-Cal outpatient claims to be HIPAA compliant during calendar year 2005. However, the State expressed the desire to initiate discussions during the summer of 2005 with the goal to target conversion of the County's Medi-Cal outpatient claims to a HIPAA compliant format sometime during calendar year 2006. On June 6, 2005, DHS contacted the State to inquire about a timetable for discussing this issue. The State indicated that they are reviewing the issue and will contact DHS once a determination has been made.
- **HIPAA Compliant Encounter Records.** The Office of Managed Care (OMC) and DHS hospitals continue to work with LACare to submit HIPAA compliant encounter records from our hospitals to OMC and then to LACare. OMC reported that the last file submitted to LACare passed their front end claims processing cycle and edits. Accordis has begun work on Phase II of the project in which the ancillary CPT-4 codes and ICD-9 codes (if available on the Affinity system) will be included on the file sent to OMC. Accordis anticipates submitting the first file under Phase II by the end of the month for OMC's review.
- **Inpatient Mental Health Services Claiming.** Three of the four DHS hospitals utilize the non-HIPAA compliant, legacy Mental Health Management Information System (MHMIS) to submit mental health services claims for both Medi-Cal and Short Doyle reimbursement. Currently, Harbor/UCLA Medical Center (HUCLA) is piloting the HIPAA compliant DMH IS and is experiencing problems using the IS to submit completed psychiatric claims to the State. Meetings have been held with the IS vendor, Sierra Systems, Inc. (Sierra) and DMH to address system claiming issues and reporting needs, and substantial progress has been made. However, HUCLA still requires some key issues to be resolved in order to be fully functional under the new IS system.

Department of Mental Health and Kirby Center

- **HIPAA Compliant Medi-Cal Outpatient Claims.** DMH has been producing HIPAA compliant claims for outpatient services provided by directly operated clinics and contracted providers. DMH has returned to near routine processing of Medi-Cal claims. Claim submission is slowed by the IS processing capacity, which limits how quickly claims files can be produced without seriously impacting system performance. DMH, Sierra, and the Internal Services Department are working together to make changes to the IS configuration to improve the speed of claims processing without negatively impacting IS users.

DMH and Sierra are providing technical assistance to providers who have a high number of denied claims or have otherwise been unsuccessful in processing claims through the IS. DMH has provided advanced IS training for providers to further assist them in resolving and resubmitting denied claims.

DMH will continue to submit claims for outpatient services provided by Fee-for-Service (FFS) contractors through the legacy FFS claiming system in a non-HIPAA compliant format, until existing IS performance and functionality issues are resolved. This work-around has reduced the delays in claim submissions and payments.

- **HIPAA Compliant Medi-Cal Inpatient Claims.** DMH is current with the submission of Medi-Cal inpatient claims to the State. As reported above, DMH continues to work with HUCLA to identify and address issues related to establishing and sustaining accurate claiming at HUCLA.
- **HIPAA Compliant Medicare Claims.** DMH and Sierra have submitted HIPAA-compliant claims to Medicare, but with mixed success. Claims have been accepted and processed, only to lead to difficulties getting a remittance advice (payment) file that DMH and Sierra can process. Medicare claims have been held since January 2005 in order for Sierra to make changes to the code that generates the outbound 837 claims for Medicare to incorporate the claim identification number, the service units, and some additional changes. If testing goes well, DMH plans to deploy these changes in two weeks. Immediately following deployment, Sierra will generate the first batch of Medicare claims directly out of the IS, without the involvement of the legacy MHMIS. If successful, this will be an important step forward in simplifying the Medicare claims submission process and may be leveraged to improve inpatient Medi-Cal claims.
- **Integrated System Improvements.** DMH and Sierra have met in the wake of the DMH rejection of Change Request (CR) 33, once seen as a key element in the IS Improvement Plan, to discuss how to accomplish the more important goals of CR 33 at a lower cost, lower risk, and with a shorter delivery time. Sierra reports that they are working on designing a more sharply focused change that would be a significant step forward, but less ambitious, and therefore involve less risk, than CR 33. Additionally, there is considerable work being done on various portions of the IS hardware configuration to improve both performance and reliability, which should result in a series of incremental improvements over some months.

- **Late Claims.** On June 8, 2005, the State Department of Health Services notified DMH that it has agreed to pay claims submitted to the State Department of Mental Health after the claims submission deadline for the period February 2004 through September 2004 because of HIPAA implementation issues. The estimated value of these claims is at least \$8.0 million.

Security Rule Compliance Issues

- **HIPPA Security Risk Analysis.** The security analysis will identify gaps between the HIPAA Security Rule practices and requirements based on each covered department's current security practices and makes recommendations for improvement. The table below identifies some of the gaps common to covered departments by security rule category.

Administrative Safeguard	Physical Safeguard	Technical Safeguard
▪ Additional security awareness training for system administrator	▪ Improve communications between information technology and facilities personnel related to HIPAA security protection needs	▪ Lack of well stated technical requirements are needed to support administrative and physical requirements
▪ Lack of security management plans that identify security roles and responsibilities and apply security standards	▪ Data Centers varied in their adherence to security best practices	▪ Technical tools need to be configured to support administrative safeguards such as password controls and automatic lockout
▪ No established metrics to measure security program effectiveness		▪ Information Technology hardware standards are lacking
▪ Inconsistent practices for the termination of employees and information access		
▪ Lack of portable device protective measures		
▪ Improve controls and documentation of production system emergency changes		
▪ Need periodic vulnerability assessments of network and server applications		

To expedite compliance efforts, covered departments were briefed on the risk analysis findings and given full draft reports, identifying high-risk issues and recommendations for improvement. These departments have already addressed some high-risk issues, including desktops and servers with EPHI access that lacked adequate password protections and servers that were susceptible to malicious attack.

Final report recommendations, ranked by criticality, will identify controls required to mitigate or reduce potential vulnerabilities and will be the basis for department risk mitigation plans.

- **DHS Increased HIPAA Risk Analysis Scope.** As reported previously, the Information Technology Software Services Master Agreement (ITSSMA) Work Order for FOX was amended on May 15, 2005 to include the complete assessment (administrative, technical, and physical) of the Office of Managed Care (OMC) and to address additional technical assessments of 16 DHS facilities. This Amendment will ensure a more comprehensive risk analysis for DHS. Fox has completed its analysis work and will be providing preliminary reports on OMC in mid-July and the facility technical assessments in late-July for DHS review. A final report is scheduled to be completed in mid-August.
- **Management of Remediation Activities.** My office will be working with covered departments to develop risk mitigation plans to implement the risk analysis recommendations. We will be monitoring progress in bi-weekly meetings held by the CISO, which will continue indefinitely until significant risk remediation compliance is achieved. The Auditor-Controller has recently appointed a HIPAA Privacy Officer, Linda McBride, who participates in these meetings to ensure that privacy issues are addressed.
- **Enterprise Security Solutions.** My office will continue to identify and implement countywide information security solutions to assist the covered components in complying with items specified in the HIPAA Security Rule. These include:
 - Network tool sets for intrusion detection and policy compliance
 - Information security awareness program for all County departments
 - Secure instant messaging
 - Network access controls for all external and internal network connections
 - Vulnerability assessment software
 - Encryption services for transmitted data
 - Cyber alerts, including anti virus patching and versioning
 - CSIRT incident response team
 - Disaster recovery and business continuity

Should you have any questions, please call me at (213) 974-2008 or Jonathan Williams, Chief Deputy, at (213) 974-2080.

JWF:GM:sjc

Attachment

c: Department Heads
Chair, Information Systems Commission

Los Angeles County
Summary HIPAA Transactions and Code Sets Status

Organization	Transactions	Compliance Strategy	County Complete & Ready To Test With Trading Partner	Trading Partner Testing Complete	Transaction in Production Use	Comments
	Health Care Claim (837) Outbound	Outsource to Clearinghouse (Accordis)		Inpatient - Yes Outpatient - No	Inpatient - Yes Outpatient - No	Accordis (DHS Clearinghouse) is submitting Medicare inpatient and outpatient 837 claims using approved HIPAA compliant Transaction Code Sets (TCS) information reflective of all-inclusive rate revenue codes. Accordis is submitting HIPAA-compliant Medicare non-hospital 837 claims to the Fiscal Intermediary (NHIC).
DHS Hospitals and Associated Clinics						Accordis is submitting HIPAA-compliant Inpatient Medi-Cal claims with "from" service dates beginning February 1, 2004 through the Medi-Cal Fiscal Intermediary (EDS). On December 2, 2004, the State indicated that they will not be converting the Medi-Cal outpatient claims to be HIPAA compliant during calendar year 2005. However, the State would like to initiate discussions on this issue during the summer of 2005 in order to convert the Medi-Cal outpatient claims sometime during calendar year 2006. On June 6, 2005, DHS contacted the State and asked if there was a timetable for discussing this issue. The State indicated that they would review the issue and get back to us.
	Health Care Claim (837i) Outbound	Outsource to Clearinghouse (Accordis)				DHS is submitting HIPAA 837 encounter data, via its clearinghouse (Accordis), to OMC. The encounter data submitted is consistent with the data required by the CDHS in processing Inpatient Medi-Cal fee-for-service claims and claims submitted to other health plans. OMC has submitted the DHS data to LACare and the file passed LACare's front end claims processing cycle and edits. Accordis has begun work on Phase II of the project to include the ancillary CPT-4 codes and ICD-9 codes, if available on the Affinity system on the file sent to OMC. Accordis anticipates submitting the first file under Phase II by the end of the month for OMC's review.
	Remittance Advice (835)	Outsource to Clearinghouse (Accordis)				The test file submitted by the contracted vendor has been approved by ISD. The Medicare fiscal intermediary was notified to begin sending the remittance advice (RA) data in the HIPAA compliant format by no later than June 13, 2005. For HIPAA security reasons, the RA information will be transmitted by the contracted vendor to Health Services Administration (HSA) and stored on a server. The facilities will retrieve the RA information from the HSA server.
		QuadraMed Affinity/Provider Advantage 270/271				The State has announced that as of July 1, 2005, they will no longer accept non-HIPAA compliant 270 eligibility inquiries. Since the Online Eligibility System (OES) does not meet HIPAA requirements, the State has indicated that they will no longer accept and process OES inquiries as of July 1, 2005. Since the State has updated their Point-of-Service (POS) system to meet HIPAA requirements, the County will utilize this system, as well as other systems (e.g., Provider Advantage VeriLink, etc.) for obtaining Medi-Cal eligibility information. For business purposes, DHS has installed the necessary software at all facilities to process HIPAA compliant 270/271 transactions (i.e., Provider Advantage VeriLink). The software is in production and HIPAA compliant 270/271 transactions are being processed to various third party payors including Medi-Cal and Medicare. The Department has met the State's November 20, 2004 "go live" date for accepting HIPAA compliant 270/271 transactions.
	Health Care Claim (837) Outbound	Outsource to Clearinghouse (Accordis)				The administrative code sets were implemented as scheduled on October 16, 2003. Claims with service dates of September 22, 2003 and greater were submitted to the State and have been adjudicated.
DHS Public Health Clinics						With regards to the implementation of national code sets, the State has not provided instructions on how to convert the local revenue codes to national codes. Therefore, until the information is received from the State, the clearinghouse vendor, Accordis, is unable to comply with HIPAA TCS regulations. Testing for format has been completed with the State and Accordis has received notification that it passed all format testing.
	Remittance Advice (835)	Paper				No change to existing process.
DHS Alcohol and Drug Programs Administration	Health Care Claim (837) Outbound	Custom coded front-end upgrade to capture the HIPAA data elements. Accordis, a clearinghouse, will process the actual transaction.				DHS Alcohol and Drug Programs Administration (ADPA) is submitting HIPAA-compliant 837 claims transactions to the State Department of Alcohol and Drug Programs (SADP) through its clearinghouse vendor, Accordis.
	Health Care Claim (837) Inbound	Paper				No change to existing process.
	Remittance Advice (835)	Paper				No change to existing process.
	Remittance Advice (835) Inbound	Paper				No change to existing process for the time being. The State has not provided a date by which they will implement a HIPAA compliant remittance advice (835) transaction.

Los Angeles County
Summary HIPAA Transactions and Code Sets Status

Organization	Transactions	Compliance Strategy	County Complete & Ready To Test With Trading Partner	Trading Partner Testing Complete	Transaction in Production Use	Comments
DHS Office of Managed Care (OMC)	Health Care Claim (837) Inbound	Vendor (HMS) modifying PMS to accept HIPAA compliant claim transactions from out-of-plan providers.				The X.12 837 transaction is certified by Claredi, however no trading partners have contacted CHP to conduct HIPAA-compliant transactions. OMC will continue processing this transaction in pre-HIPAA format consistent with the contingency plan, or on paper, until trading partner testing is complete. DHS has completed setting up a virtual private network with Claimsnet and OMC has completed system testing with Claimsnet. OMC continues outreach efforts to identify potential trading partners with out-of-network hospitals and physicians with whom to begin testing. No negative impact to OMC business processes or revenue flow has occurred. Status changed from "Not complete" to "Not complete for reasons beyond the control of the County" because CHP is technically ready to receive a 837 I&P should one be sent.
	Health Care Encounter (837) Inbound	Interface engine software being installed to feed the OMC Data Warehouse. Using clearinghouse (DDD) to translate incoming proprietary format from non-County providers to HIPAA-compliant 837 format.				OMC is accepting HIPAA-compliant 837P transactions from non-County providers via a clearinghouse (DDD) and they are testing the 837I. OMC is evaluating the transactions from DHS hospitals transmitted through Accordis. Please refer to the "Health Care Claim (837I) Outbound" status in the above "DHS Hospitals and Associated Clinics" section.
						OMC has modified its legacy system to process the transactions between DHS hospitals and OMC until the production server and the new interface engine is installed and completely tested. OMC is currently configuring the interface engine that will allow receipt of HIPAA-compliant 837I encounter records from DHS hospitals and will replace the interim solution now being tested.
	Health Care Encounter (837) Outbound	Data extracted from Data Warehouse will feed translator software to produce HIPAA compliant transactions.				CHP is fully compliant on the submission of non-County provider transactions via a clearinghouse (DDD). No negative impact on business processes or revenue flow is anticipated.
	Remittance Advice (835) Outbound	Vendor (HMS) modified PMS to produce HIPAA compliant transactions.				The X.12 835 transaction is certified by Claredi, but it has not yet been tested with trading partners and no trading partner has requested remittance advice information in electronic format. OMC is currently providing 835 equivalent information on paper to its trading partners. HIPAA compliance is a non-issue until a switch is made to an electronic transaction. No negative impact on business processes or revenue flow has occurred.
Office of Managed Care (OMC)	Health Care Enrollment and Disenrollment (834)	Vendor (HMS) modified PMS to produce HIPAA compliant transactions.				OMC was able to process a compliant X.12 834 transaction as of the October 16, 2003 deadline. DHS currently provides its eligibility roster electronically to certain plan providers, including DHS facilities. OMC is in production with processing the Healthy Families' new data vendor, Maximus, and is also in production with LA Care, for Medi-Cal and will be in production March 2005.
	Premium Payment Order/ Remittance Advice (820)	Vendor (HMS) modifying PMS to accept and translate HIPAA transactions.				The State Healthy Families Program (HFP) is not expected to be ready to test the X.12 820 transaction with trading partners until the spring of 2005. HFP stated that the 820 electronic file they currently distribute is "materially compliant." The necessity for OMC to receive an X.12 820 transaction is settled and the need to generate an outbound 820 is still being investigated. OMC has completed custom programming modifications to its Patient Management System (PMS) that will allow it to receive and process the inbound 820 transaction, but has reached a point where they can make little progress without more information from the State. OMC will convert the 820 transaction file received from HFP to a flat file that will be sent to OMC Finance, thus mitigating any negative impact on OMC Finance or County Treasurer and Tax Collector (TTC) operations. In the interim, DHS will continue to process transactions in pre-HIPAA format. No negative impact on business processes or revenue flow is anticipated.
						OMC is ready to receive a 270 and return a 271. Trading partners have been contacted, but to date no providers have expressed an interest in using these transactions, and those that are interested do not yet meet the OMC's minimum trading partner requirements. Hence there has been no testing with trading partners. No negative impact on business processes or revenue flow has occurred.
	Claim Status Summary (276/277)	Vendor (HMS) modified PMS to produce HIPAA compliant transactions.				OMC is ready to receive a 276 and send a 277. Trading partners have been contacted, but to date no providers have expressed an interest in using these transactions; hence there has been no testing with trading partners. No negative impact on business processes or revenue flow has occurred.
	Health Care Service Review (278)	Vendor (HMS) modified PMS to produce HIPAA compliant transactions.				OMC is ready to receive and send a 278. Trading partners have been contacted, but to date no providers have expressed an interest in using these transactions; hence there has been no testing with trading partners. No negative impact on business processes or revenue flow has occurred.
	NCPDP	Pharmacy Benefit Management Contractor				Contractor (PCN) is responsible for HIPAA compliance of NCPDP transactions.

Los Angeles County
Summary HIPAA Transactions and Code Sets Status

Organization	Transactions	Compliance Strategy	County Complete & Ready To Test With Trading Partner	Trading Partner Testing Complete	Transaction in Production Use	Comments
DHS California Children's Services	Health Care Claim (837) Outbound	In-house development of 837 transaction output				Completed. Process is now routine.
	Health Care Claim (837) Inbound	Paper				No change to existing process.
	Remittance Advice (835)	Vendor (EDS) supplied via website				Completed. Process is now routine.
	NCPDP	Paper				No change to existing process.
	Health Care Claim (837)	Integrated System - Wrapper of MHMIS and FFS (EDS)				No change. The Health Care Claim (837) is in production use, however some claims are still sent to the State in legacy format while IS performance and functionality issues are resolved.
DMH Department of Mental Health	Health Care Enrollment and Disenrollment (834)	Integrated System - Wrapper of MHMIS and FFS (EDS)				No change from last report. DMH began using the Integrated System (IS) to exchange the X.12.834 HIPAA transaction with Fee-for-Service Network Providers on November 24, 2003. DMH began using the Integrated System (IS) to exchange the X.12.834 HIPAA transaction with Short-Doyle providers on February 9, 2004. State and Federal compliance status is not relevant to or a constraint on this transaction.
	Remittance Advice (835) Inbound	Integrated System - Wrapper of MHMIS and FFS (EDS)				The State is now sending HIPAA compliant remittance advice transactions to DMH and they are being processed in the IS. For a time DMH had a backlog of these transactions awaiting loading into the IS, but the back log has been processed. The status of this transaction has been upgraded from "yellow" to "green" since it now appears to be the routine way of conducting this transaction.
	Remittance Advice (835) Outbound	Integrated System - Wrapper of MHMIS and FFS (EDS)				No change from last report. DMH pays for some services directly to the provider and for those services on the IS, they are currently producing HIPAA compliant X.12.835 remittance advice transactions within the IS. One contract provider is sending 837 transactions via EDI and Sierra returns the compliant 835 by EDI. FFS providers do not yet receive a HIPAA-compliant X.12.835 for approved claims since their claims are still sent to the State in a non-compliant format. They receive HIPAA compliant 835's for denied claims within the IS. While this transaction is in production use, its status is "yellow" because some significant trading partners are not involved at this time.
	Eligibility Inquiry & Response (270/271)	Integrated System - Wrapper of MHMIS and FFS (EDS)				The State is now offering the opportunity to test the HIPAA compliant 270/271 transaction. DMH has asked the State to validate a reported implementation deadline of July 1, 2005. This is an unrealistic deadline for DMH.
	Authorization (278)	Integrated System - Wrapper of MHMIS and FFS (EDS)				No change from last report. The Integrated System began processing X.12.278 transactions internally with Fee-for-Service network providers on November 24, 2003. State Medi-Cal will not support compliant authorization transactions this year. DMH will continue to process transactions in a pre-HIPAA format with the State in the meantime. While this transaction is in production use, its status is "yellow" because of the limited number of trading partners involved at this time and the limited manner in which it is used.
NCPDP	Health Care Claim Status Summary (276/277)	Integrated System - Administrative Transactions				No change from last report. DMH is presently offering the 276 and 277 X.12 transactions to Fee-for-Service network providers and Short-Doyle contract providers who are sending HIPAA compliant claims via EDI, but it is not a transaction currently used. State Medi-Cal will not support compliant status reporting transactions this year.
	NCPDP	Integrated System - Wrapper of MHMIS				No change from last report. The HIPAA-compliant NCPDP transaction became available for production use on February 9, 2004. No pharmacy providers are testing or using IS pharmacy functionality in production. Changes to the Pharmacy IS Deployment Plan have been identified, but not formally documented. The documentation effort is on hold until more pressing IS issues are resolved. This is expected to have no negative impact on pharmacy providers.

LEGEND

























COMPLETE

NOT COMPLETE FOR REASONS BEYOND COUNTY CONTROL

NOT COMPLETE

STATUS BY HIPAA SECURITY RULE STANDARD

ADMINISTRATIVE SAFEGUARDS

Standards	Description	County Covered Components				Status
		DHS	DMH	LASD	Kirby	
Security Management Process 164.308(a)(1)	Implement processes and procedures to manage HIPAA Security including risk analysis and remediation.					The County has contracted with Fox Systems Inc. to complete the Risk Analysis that is required by HIPAA by June 15, 2005. Some risk remediation activities have already occurred, but other activities will be identified following the completion of risk analysis.
Assigned Security Responsibility 164.308(a)(2)	Identify a security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.					The County has appointed a Chief Information Security Officer with responsibility for HIPAA security implementation. The covered components have also appointed departmental security officers to oversee these processes within their respective organizations.
Workforce Security 164.308(a)(2)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.					DMH policies and procedures are complete. While the Sheriff's Pharmacy function has developed policies, procedures must still be written and implemented.
Information Access Management 164.308(a)(4)	Implement policies and procedures for authorizing access to electronic protected health information.					Sheriff's Pharmacy function has written policies, but has not developed procedures to implement them.
Security Awareness and Training 106.308(a)(5)	Implement a security awareness and training program for all members of its workforce (including management).					Initial security awareness training has been completed for all of the covered components. The current training activity is ongoing as needed to train all new staff and to augment that training for all staff related to policy requirements.
Security Incident Procedures 106.308(a)(6)	Implement policies and procedures to address security incidents.					This particular standard does not apply to Probation Department's Kirby Center, which relies on systems that are owned and maintained by DMH. The other covered components have developed policies and procedures to respond to security incidents, but have not designated and trained teams to conduct investigations.



COMPLETED















IN PROGRESS



NOT STARTED

STATUS BY HIPAA SECURITY RULE STANDARD

ADMINISTRATIVE SAFEGUARDS					
Standards	Description	County Covered Components			
		DHS	DMH	LASD	Kirby
Contingency Plan 106.308(a)(7)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.				
Evaluation 164.308(a)(8)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information.				
Business Associate Contracts and Other Arrangement 164.308(b)(1)	Written contract or other arrangement (Memorandum of Understanding) between covered entity and its business associate representing that the business associate is in compliance with HIPAA Security Rule safeguards.				
		Status			
		Contingency planning is in process for all of the covered components, but has not been completed or tested. Application criticality analysis has not been started for any of the covered components. Probation Department's Kirby Center, which relies on systems that are owned and maintained by DMH, is required to develop an emergency mode of operations plan.			
		The evaluation process is an ongoing task that is required as part of being HIPAA compliant. Timing of activities within this standard is dependent on system changes that may affect the risk electronic protected health information over time.			
		All of the 386 Business Associate (BA) agreements and 19 Memorandums of Understanding (MOU) have been completed and sent to the required entities. The covered departments have received 240 signed BA agreements and 17 MOUs.			



COMPLETED



















IN PROGRESS



NOT STARTED

STATUS BY HIPAA SECURITY RULE STANDARD

PHYSICAL SAFEGUARDS						
Standards	Description	County Covered Components				Status
		DHS	DMH	LASD	Kirby	
Facility Access Controls 164.310(a)(1)	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.					Facility access policies have been developed and implemented. However, all of the covered components must develop facility security plans and procedures to maintain maintenance records for facility security systems.
Workstation Use 164.310(c)	Procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.					DMH policies and procedures have been implemented. While the Sheriff's Pharmacy function has developed policies, procedures are still being written and implemented.
Workstation Security 164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.					Sheriff's Pharmacy function has developed policies, but procedures must still be written and implemented.
Device and Media Controls 164.310(d)(1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.					Sheriff's Pharmacy function has developed policies, but procedures must still be written and implemented.



COMPLETED























IN PROGRESS



NOT STARTED

STATUS BY HIPAA SECURITY RULE STANDARD

TECHNICAL SAFEGUARDS

Standards	Description	County Covered Components				Status
		DHS	DMH	LASD	Kirby	
Access Control 164.312(b)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.					Policies have been developed, however individual systems must be identified and reviewed to ensure compliance.
Audit Controls 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.					The covered components have developed policies, but have not implemented audit controls on all systems that provide reports on access attempts that are reviewed periodically. Probation's Kirby Center relies on systems that are owned and maintained by the Department of Mental Health who is responsible for developing and maintaining audit trails on their systems.
Integrity 164.312(c)(1)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.					Sheriff's Pharmacy function has developed policies, but procedures must still be written and implemented.
Person or Entity Authentication 164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.					Sheriff's Pharmacy function has developed policies, but procedures must still be written and implemented.
Transmission Security 164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.					All of the covered components have developed policies to require encryption of sensitive data. However, no specific solutions have been implemented. E-mail transmissions may need encryption, but results of the risk analysis are required to determine what is actually required.

P:\Drafts\HIPAA\2005 BOS Status\detailhippasecuritystatus_June2005.doc



COMPLETED



IN PROGRESS



NOT STARTED